Journal of Algebra 322 (2009) 1974–1978

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Seminormality and polynomial rings

Sami Barhoumi

Équipe de Mathématiques, UMR CNRS 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25030 Besancon cedex, France

ARTICLE INFO

Article history:
Received 8 August 2008
Available online 18 July 2009
Communicated by Michel Broué

Keywords:
Seminormality
Constructive mathematics
Computer algebra

ABSTRACT

We give a direct algorithmic proof of the implication "**A** seminormal implies $\mathbf{A}[X]$ seminormal".

1. Introduction

In [2] T. Coquand obtained a constructive proof of the following theorem [6,7].

Theorem 1 *(Traverso–Swan–Coquand). Let k be a positive integer. A reduced ring* **A** *is seminormal if and only if the canonical map* $\operatorname{Pic}\mathbf{A} \to \operatorname{Pic}\mathbf{A}[X_1, \ldots, X_k]$ *is an isomorphism.*

Recently we have obtained in a joint paper with H. Lombardi an algorithmic proof for the "if part" in the one variable case [1]. The "only if part" is based on a Schanuel's example. In this paper, using the same philosophy as in [1], we give a direct algorithmic proof of the following corollary of Theorem 1.

Corollary 2. *If a ring* **A** *is seminormal then so is* $\mathbf{A}[X]$.

Combined with [1] (i.e., Theorem 1 when $k = 1$), this gives an algorithm for Theorem 1 by induction on k.

We recall [6] that a ring **A** is seminormal if when $b^2 = c^3$ then there exists $a \in \mathbf{A}$ such that $b = a^3$ and $c = a^2$. A seminormal ring is reduced.

E-mail address: sami.barhoumi@univ-fcomte.fr.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2009.06.013

When $\mathbf{A} \subseteq \mathbf{B}$ are commutative rings, the *seminormal closure* of $\mathbf{A}$ in $\mathbf{B}$ is the smallest subring $\mathbf{A}_1$ of $\mathbf{B}$ containing $\mathbf{A}$ such that if $x \in \mathbf{B}$, $x^2 \in \mathbf{A}_1$ and $x^3 \in \mathbf{A}_1$ then $x \in \mathbf{A}_1$.

A reduced zero-dimensional ring (often called von Neumann regular) is a slight generalization of a field. For any element x there exists a quasi-inverse y: $x^2y = x$ and $xy^2 = y$. Then $e_x = xy$ is idempotent and $1 - e_x$ generates the annihilator of x.

Lemma 3. *If $\mathbf{A}$ is a reduced ring then $\mathbf{A}$ has a reduced zero-dimensional extension $\mathbf{C} \supseteq \mathbf{A}$.*

Remark. If $\mathbf{A}$ is an integral domain, then it suffices to get $\mathbf{C}$ its fraction field.

Fact 4. Let us start with an arbitrary reduced ring $\mathbf{A}$ contained in a reduced zero-dimensional ring $\mathbf{C}$. Assume that we have $f_2, f_3 \in \mathbf{A}[X]$ with $f_2^3 = f_3^2$. Then there exists $f \in \mathbf{C}[X]$ such that $f^2 = f_2$ and $f^3 = f_3$.

Proof. This is clear if $\mathbf{C}$ is a field since f can be obtained as the Euclidean quotient of f^3 by f^2.

In the general case, the result is also true because a reduced zero-dimensional ring behaves like a field in any computation, up to the fact we have to replace the disjunction "$u = 0$ or u is invertible" (each time this kind of disjunction appears in an algorithm) by the splitting of $\mathbf{C}'$ as $\mathbf{C}' \simeq \mathbf{C}'/\langle e_u\rangle \times \mathbf{C}'/\langle 1 - e_u\rangle$, where e_u is the idempotent annihilator of u. In $\mathbf{C}'/\langle e_u\rangle$, u is invertible, and in $\mathbf{C}'/\langle 1 - e_u\rangle$, $u = 0$. □

Context: Let $\mathbf{C}$ be a ring and $f = a_0 + a_1X + \cdots + a_dX^d$ polynomial in $\mathbf{C}[X]$. Let $\mathbf{A}$ be the ring generated by the coefficients of f^2 and f^3. Let $\mathbf{B}$ be the ring generated by the coefficients of f. We denote by $\mathbf{A}_1$ the seminormal closure of $\mathbf{A}$ in $\mathbf{B}$.

It is clear from Lemma 3 and Fact 4 that Corollary 2 is a consequence of the following more precise statement.

Theorem 5. *Within Context we get $\mathbf{A}_1 = \mathbf{B}$. More precisely there are finitely many elements $c_1, \ldots, c_m \in \mathbf{B}$ such that $c_{i+1}^2, c_{i+1}^3 \in \mathbf{A}[c_1, \ldots, c_i]$ $(i \in \{1, \ldots, m-1\})$ and $\mathbf{B} = \mathbf{A}[c_1, \ldots, c_m]$.*

In Section 3 we explain how to get algorithmically Theorem 5. In Section 2 we give some preliminary lemmas for this construction.

2. Preliminary lemmas

Lemma 6. *Within Context, the coefficients of f are integral over $\mathbf{A}$. So $\mathbf{B}$ is finite as an $\mathbf{A}$-module.*

Proof. Indeed, if u is a coefficient of f, it follows from $f \times f = f^2 \in \mathbf{A}[X]$ that u^2 is integral over $\mathbf{A}$. This is a consequence of Kronecker's theorem [3–5] that states that if $P_1P_2 = Q \in \mathbf{A}[X]$ then any product u_1u_2, where u_i is a coefficient of P_i, is integral over the ring generated by the coefficients of Q. This implies that u is integral over $\mathbf{A}$. □

Lemma 7. *Let $c \in \mathbf{B}$ and $m \in \mathbb{N}$ such that $c^n \in \mathbf{A}_1$ for any $n \geqslant m$, then $c \in \mathbf{A}_1$.*

Proof. For example let $m = 2^4 = 16$. We have: since c^{16} and $c^{24} \in \mathbf{A}_1$ then $c^8 \in \mathbf{A}_1$, since c^{18} and $c^{27} \in \mathbf{A}_1$ then $c^9 \in \mathbf{A}_1$, and so on for any $n \geqslant 8$, $a^n \in \mathbf{A}_1$. Briefly we can pass from 2^4 to 2^3. In the same way we pass from 2^3 to 2^2, and from 2^2 to 2. Thus c^2 and $c^3 \in \mathbf{A}_1$, so $c \in \mathbf{A}_1$. □

Lemma 8. *If $t \in \mathbf{A}$ and $tf \in \mathbf{A}[X]$ then there exists $k \in \mathbb{N}$ such that $t^k\mathbf{B} \subseteq \mathbf{A}$.*

Proof. We have $\mathbf{B} = \mathbf{A}[a_0, \ldots, a_d]$ where $f = a_0 + a_1X + \cdots + a_dX^d$. Every a_i is integral over $\mathbf{A}$. Let d_i be the degree of an integral dependence relation of a_i. Then $\mathbf{B} = \sum \mathbf{A}a^\delta$, with $a^\delta = a_0^{\delta_0} \ldots a_d^{\delta_d}$, $0 \leqslant \delta_i < d_i$ (δ means $\delta_0, \ldots, \delta_d$ and a^δ is a pure notation). If $tf \in \mathbf{A}[X]$ and $\sum(d_i - 1) = k$, then $t^k a^\delta = (ta_0)^{\delta_0} \cdots (ta_d)^{\delta_d} \cdot t^{k-\sum \delta_i}$ with $k - \sum \delta_i \geqslant 0$. So $t^k a^\delta \in \mathbf{A}$. Thus $t^k\mathbf{B} \subseteq \mathbf{A}$. □

Lemma 9. *If $a \in \mathbf{A}$ and $a^m\mathbf{B} \subseteq \mathbf{A}$ for some $m \in \mathbb{N}$, then $a\mathbf{B} \subseteq \mathbf{A}_1$.*

Proof. For $b \in \mathbf{B}$ we have $(ab)^m\mathbf{B} \subseteq \mathbf{A}$. This implies that $(ab)^n \in \mathbf{A}_1$ for any $n \geqslant m$. Applying Lemma 7, we get $a\mathbf{B} \subseteq \mathbf{A}_1$. □

Lemma 10. *Let $a \in \mathbf{B}$ and $\ell \in \mathbb{N}$ such that $a^\ell f \in \mathbf{A}[X]$, then $\sqrt{a\mathbf{B}} \subseteq \mathbf{A}_1$.*

Proof. This follows from Lemmas 8 and 9. □

Fact 11. Let $\mathbf{C} \subseteq \mathbf{B}$ be two rings and $\mathcal{J}$ an ideal of $\mathbf{B}$. Then $\mathbf{C} + \mathcal{J}$ is a ring, $\mathcal{J}$ is an ideal of $\mathbf{C} + \mathcal{J}$, $\mathbf{C} \cap \mathcal{J}$ is an ideal of $\mathbf{C}$, and the isomorphism of $\mathbf{C}$-modules $(\mathbf{C} + \mathcal{J})/\mathcal{J} \simeq \mathbf{C}/(\mathbf{C} \cap \mathcal{J})$ is an isomorphism of rings.

Lemma 12. *With Lemma 10 hypotheses, we have $\mathbf{A} + \sqrt{a\mathbf{B}} \subseteq \mathbf{A}_1$. Let $\mathcal{J} = \sqrt{a\mathbf{B}}$,*

$$\widetilde{\mathbf{A}} = (\mathbf{A} + \mathcal{J})/\mathcal{J} \subseteq \mathbf{A}_1/\mathcal{J} \quad \text{and} \quad \widetilde{\mathbf{B}} = \mathbf{B}/\mathcal{J},$$

then $\mathbf{A}_1/\mathcal{J}$ is the seminormal closure of $\widetilde{\mathbf{A}}$ in $\widetilde{\mathbf{B}}$.

Proof. Let $\mathbf{C}$ be the seminormal closure of $\widetilde{\mathbf{A}}$ in $\widetilde{\mathbf{B}}$. We write $\mathbf{C} = \mathbf{A}_2/\mathcal{J}$ with $\mathcal{J} \subseteq \mathbf{A}_2$ as a subring of $\mathbf{B}/\mathcal{J}$. It is clear that $\mathbf{A}_1 \subseteq \mathbf{A}_2$. Let $x \in \mathbf{A}_2$ and assume first that $\bar{x}^2, \bar{x}^3 \in \widetilde{\mathbf{A}}$. Then $x^2, x^3 \in \mathbf{A}_1$, so $x \in \mathbf{A}_1$. Reasoning inductively, we replace $\mathbf{A}$ by $\mathbf{A}[x]$. Since any element in $\mathbf{C}$ can be reached in a finite number of steps, we see that $\mathbf{A}_2 = \mathbf{A}_1$. □

The concrete consequence of Lemma 12 for our computation is that, whenever we find an $a \in \mathbf{B}$ such that $a^\ell f \in \mathbf{A}[X]$ for some integer ℓ, we are allowed to replace $\mathbf{A}$ and $\mathbf{B}$ by $\widetilde{\mathbf{A}}$ and $\widetilde{\mathbf{B}}$. Indeed, it is clear that hypotheses of Context remain true for these rings, and if forthcoming computations show that the seminormal closure of $\widetilde{\mathbf{A}}$ in $\widetilde{\mathbf{B}}$ is equal to $\widetilde{\mathbf{B}}$, Lemma 12 says that $\mathbf{A}_1 = \mathbf{B}$.

In short "we are allowed to continue the computation modulo $\mathcal{J}$".

3. Proof of Theorem 5

Within Context, we consider f as being of formal degree d. Let $f = a_0 + a_1X + \cdots + a_dX^d$ be a polynomial with formal degree d. We have

$$f^2 = a_0^2 + 2a_0a_1X + \cdots + a_d^2X^{2d} = b_0 + b_1X + \cdots + b_{2d}X^{2d},$$

and

$$f^3 = a_0^3 + 3a_0^2a_1X + \cdots + a_d^3X^{3d} = c_0 + c_1X + \cdots + c_{3d}X^{3d}.$$

First remark that $a_0^2, a_0^3 \in \mathbf{A}$ and $a_0^4a_1 = b_0c_1 - b_1c_0 \in \mathbf{A}$.

Let $i \geqslant 1$. The coefficients b_{i+1} and c_{i+1} can be written as follows

$$b_{i+1} = 2a_0a_{i+1} + \alpha_i, \qquad c_{i+1} = 3a_0^2a_{i+1} + \beta_i,$$

where α_i and β_i are sums of terms of the form $s\prod_j a_j^{m_j}$, $0 \leqslant j \leqslant i$, $\sum_j m_j \leqslant 3$, $s \in \mathbb{N}$.

So we get

$$a_0^4 a_{i+1} = b_0 c_{i+1} - c_0 b_{i+1} - (b_0\beta_i - c_0\alpha_i) \quad \text{where } b_0 c_{i+1} - c_0 b_{i+1} \in \mathbf{A}.$$

For example with $d \geqslant 4$, we have

$$\begin{aligned}
f &= a_0 + a_1 X + a_2 X^2 + a_3 X^3 + a_4 X^4 + \cdots,\\
f^2 &= a_0^2 + 2a_0a_1 X + \big(2a_0a_2 + a_1^2\big)X^2 + (2a_0a_3 + 2a_1a_2)X^3\\
&\quad + \big(2a_0a_4 + 2a_1a_3 + a_2^2\big)X^4 + \cdots\\
&= b_0 + b_1 X + b_2 X^2 + b_3 X^3 + b_4 X^4 + \cdots \in \mathbf{A}[X],\\
f^3 &= a_0^3 + 3a_0^2a_1 X + \big(3a_0^2a_2 + 3a_0a_1^2\big)X^2 + \big(3a_0^2a_3 + 6a_0a_1a_2 + a_1^3\big)X^3\\
&\quad + \big(3a_0^2a_4 + 6a_0a_1a_3 + 3a_1^2a_2 + 3a_0a_2^2\big)X^4 + \cdots\\
&= c_0 + c_1 X + c_2 X^2 + c_3 X^3 + c_4 X^4 + \cdots \in \mathbf{A}[X].
\end{aligned}$$

Then $b_2 = 2a_0a_2 + a_1^2$ $(\alpha_1 = a_1^2)$, $c_2 = 3a_0^2a_2 + 3a_0a_1^2$ $(\beta_1 = 3a_0a_1^2)$,

$$b_0\beta_1 - c_0\alpha_1 = 2a_0^3a_1^2 = 2b_0b_1 \in \mathbf{A}, \quad \text{and so} \quad a_0^4 a_2 \in \mathbf{A}.$$

It follows that $b_3 = 2a_0a_3 + 2a_1a_2$ $(\alpha_2 = 2a_1a_2)$, $c_3 = 3a_0^2a_3 + 6a_0a_1a_2 + a_1^3$ $(\beta_2 = 6a_0a_1a_2 + a_1^3)$,

$$b_0\beta_2 - c_0\alpha_2 = 4a_0^3a_1a_2 + a_0^2a_1^3 \in \mathbf{A}, \quad \text{and so} \quad a_0^{14} a_3 \in \mathbf{A}.$$

We need the following lemma.

Lemma 13. *Let n_k be defined inductively by $n_1 = n_2 = 4$, $n_3 = 14$ and for $k > 3$ $n_k = 4 + 3n_{k-1}$. Then*

1. $a_0^{n_k} a_k \in \mathbf{A}$ *for all* $k \geqslant 0$,
2. $n_k \leqslant 16 \times 3^{d-3} - 2$.

Proof. We reason by induction on k. Suppose that $a_0^{n_k} a_k \in \mathbf{A}$. Since α_k and β_k are sums of terms of the form $s\prod_j a_j^{m_j}$, $0 \leqslant j \leqslant k$, $0 \leqslant m_j \leqslant 3$, $s \in \mathbb{N}$, we get $a_0^{3n_k}\alpha_k$, $a_0^{3n_k}\beta_k \in \mathbf{A}$. Thus $a_0^{3n_k+4} a_{k+1} \in \mathbf{A}$ (as $b_{k+1} = 2a_0a_{k+1} + \alpha_k$, and $c_{k+1} = 3a_0^2a_{k+1} + \beta_k$).

For the second point we have $n_k \leqslant n_d = 16 \times 3^{d-3} - 2$. □

Conclusion: When we consider the case of f with formal degree d, the constant coefficient of f, a_0, verify $a_0^{n_d} \cdot \mathbf{B} \subseteq \mathbf{A}$. This gives a first approximation of $\mathbf{A}_1$ by $\mathbf{A}' = \mathbf{A} + \sqrt{\mathcal{I}}$ where $\mathcal{I}$ is the ideal of $\mathbf{B}$ generated by the constant coefficient of f. Since we are allowed to continue the computation modulo $\mathcal{J} = \sqrt{\mathcal{I}}$, we finish the algorithm by induction on d.

Acknowledgment

I am very grateful to Henri Lombardi for many discussions on the subject of this paper.

References

[1] S. Barhoumi, H. Lombardi, An algorithm for the Traverso–Swan theorem on seminormal rings, J. Algebra 320 (2008) 1531–1542.
[2] T. Coquand, On seminormality, J. Algebra 305 (2006) 577–584.
[3] Th. Coquand, H. Persson, Valuations and Dedekind Prague theorem, J. Pure Appl. Algebra 155 (2001) 121–129.
[4] H. Edwards, Divisor Theory, Birkhäuser, Boston, MA, 1989.
[5] H. Lombardi, Hidden constructions in abstract algebra (1): Integral dependance relations, J. Pure Appl. Algebra 167 (2002) 259–267.
[6] R. Swan, On seminormality, J. Algebra 67 (1980) 210–229.
[7] C. Traverso, Seminormality and Picard group, Ann. Sc. Norm. Super. Pisa 24 (1970) 585–595.